

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-008607

(43)Date of publication of application : 10.01.2003

(51)Int.Cl.

H04L 12/46

H04L 12/56

(21)Application number : 2001-193090

(71)Applicant : NEC CORP

(22)Date of filing : 26.06.2001

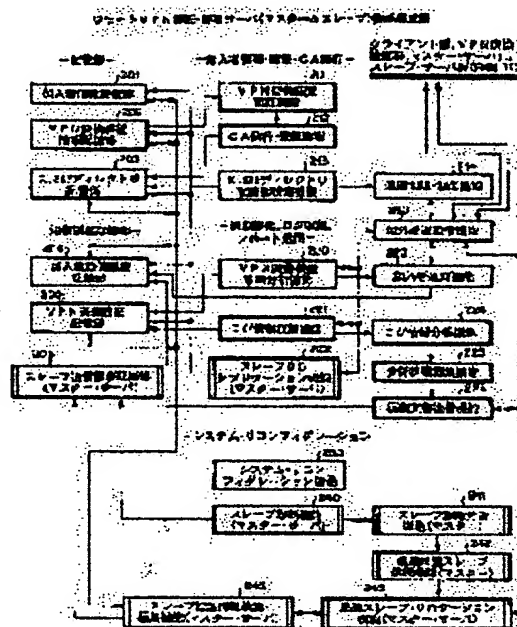
(72)Inventor : ONAWA YOICHI

(54) REMOTE VPN AUTHENTICATION AND MANAGEMENT SYSTEM, AND CONSTRUCTING METHOD OF THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide integrated virtual private network (VPN) service management and operation which have not been performed because a VPN is established, managed and operated in each link, and to provide unified tunnel server operation and management in communication with plural ISPs.

SOLUTION: In a server which is established between a group of clients and a group of Internet service providers and remotely authenticates and manages a group of VPN converters to provide end-to-end VPN service, this remote VPN authentication and management server is featured in that it has a means to issue an authentication certificate, a means to control communication, a means to collect status information, a means to collect traffic statistics information, a means to monitor and control faults, a means to analyze statistics information, and a means to report to each client.



LEGAL STATUS

[Date of request for examination]

28.05.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-8607

(P2003-8607A)

(43) 公開日 平成15年1月10日 (2003.1.10)

(51) Int.Cl.⁷

識別記号

F I

テーマコード* (参考)

H 0 4 L 12/46

H 0 4 L 12/46

M 5 K 0 3 0

12/56

4 0 0

12/56

4 0 0 Z 5 K 0 3 3

審査請求 有 請求項の数11 O L (全 14 頁)

(21) 出願番号 特願2001-193090 (P2001-193090)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(22) 出願日 平成13年6月26日 (2001.6.26)

(72) 発明者 大縄 陽一

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100065385

弁理士 山下 穰平

Fターム(参考) 5K030 GA11 GA15 HA04 JA10 MB09

MC07

5K033 BA08 DA05 DB20 EA07

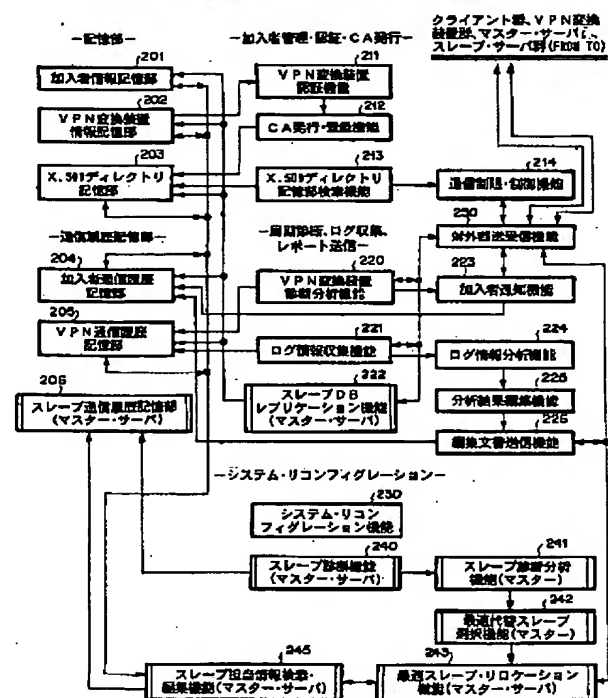
(54) 【発明の名称】 リモートVPN認証・管理システムおよびリモートVPN認証・管理システム構築方法

(57) 【要約】

【課題】 VPNはリンク・バイ・リンクで設定され管理運用される為、統合的VPNサービスの管理運営が成されないという問題と複数のISPにまたがる通信においては、トンネルサーバの運営管理が一元的に成されていないという問題があった。

【解決手段】 クライアント群とISP (internet service provider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群をリモートから認証・管理サービスを提供するサーバにおいて、認証証発行手段と、通信を制御する手段と、ステータス情報収集手段と、トラフィック統計情報収集手段と、障害監視制御手段と、統計情報分析手段と、各クライアントにレポート手段と、を備えることを特徴とするリモートVPN認証・管理サーバの提供。

リモートVPN認証・管理サーバ(マスター&スレーブ)機能構成図



【特許請求の範囲】

【請求項1】 クライアント群とISP (internet service provider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群をリモートから認証・管理サービスを提供するサーバにおいて、前記クライアント群からのサービス提供への加入申請情報を受付・審査後、審査結果を前記クライアント群に通知する手段と、前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第1の記憶部に前記クライアント毎に登録する手段と、前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記VPN変換装置群の情報を前記第1の記憶部に前記クライアント毎に登録する手段と、前記登録されたクライアント群との通信内容の履歴を第2の記憶部に前記クライアント毎に登録する手段と、前記登録されたVPN変換装置との通信内容の履歴を第3の記憶部に前記VPN変換装置毎に登録する手段と、前記加入登録されたクライアントが加入申請時、通信宛先の情報を申請した場合、通信宛先情報を第4の記憶部に前記クライアント毎に登録する手段と、前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記VPN変換装置群に認証証を発行する手段と、前記認証証が発行されたVPN変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第4の記憶部に前記クライアント毎に登録された通信宛先情報を検索する手段と、前記検索結果を前記VPN変換装置群に通知する手段と、前記認証証が発行されたVPN変換装置群からステータス情報を収集する手段と、前記認証証が発行されたVPN変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集する手段と、前記認証証が発行されたVPN変換装置群に所定周期のプロブを送信し障害の監視制御を行う手段と、前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析する手段と、前記分析結果を前記認証証が発行された前記各クライアント群にレポートする手段と、を備えることを特徴とするリモートVPN認証・管理サーバ。

【請求項2】 WWWブラウザを具備したクライアント群とISP (internet service provider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群

をリモートから認証・管理サービスを提供するシステムにおいて、

前記クライアント群からのサービス提供の加入申請を受付・審査後、前記審査結果を前記クライアント群に通知する手段と、

前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第1の記憶部に前記クライアント毎に登録する手段と、

前記審査結果でサービス可能と判定された前記クライアント群が使用する前記VPN変換装置群の情報を前記第1の記憶部に前記クライアント毎に登録する手段と、

前記登録されたクライアント群との通信内容の履歴を第2の記憶部に前記クライアント毎に登録する手段と、

前記登録されたVPN変換装置群との通信内容の履歴を第3の記憶部に前記VPN変換装置毎に登録する手段と、

前記クライアント群が加入申請時に申請した通信アクセス宛先情報を記憶する第4の記憶部に前記クライアント毎に登録する手段と、

前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記VPN変換装置群に認証証を発行する手段と、

前記認証証が発行されたVPN変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第4の記憶部に前記クライアント毎に登録された前記通信宛先情報を検索する手段と、

前記検索結果を前記認証証が発行されたVPN変換装置群に通知する手段と、

前記認証証が発行されたVPN変換装置群からステータス情報を収集する手段と、

前記認証証が発行されたVPN変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集する手段と、

前記認証証が発行されたVPN変換装置群に所定周期のプロブを送信し障害の監視制御を行う手段と、

前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析する手段と、

前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポート情報を編集する手段と、

前記所定周期で編集した文書情報を電子メールにハイパーリンクする手段と、

前記電子メールに前記第1の記憶部にある前記クライアント群のメールアドレスを付加する手段と、

前記電子メールを所定周期で送信する手段と、

前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポート内容が表示される手段と、

を備えることを特徴とするリモートVPN認証・管理サ

ーバ。

【請求項 3】 請求項 2 に記載のリモート V P N 認証・管理サーバにおいて、
地理的条件と前記認証証が発行された V P N 変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散システム構成とする手段と、
前記マスター・サーバで前記マスター・サーバと前記スレーブ・サーバ群との通信の履歴を第 5 の記憶部に前記スレーブ・サーバ毎に登録する手段と、
前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証する手段と、
前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバで前記ワン・タイム・パスワードで認証する手段と、
前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバがあった場合、前記マスター・サーバにおいて最適代替スレーブ・サーバの選択手段と、
前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象とする前記認証証が発行された V P N 変換装置に関する前記第 1 の記憶部、第 2 の記憶部、第 3 の記憶部および第 4 の記憶部の関連情報を送信し確認応答をとる手段と、
前記スレーブ・サーバ群には、前記第 1 の記憶部、第 2 の記憶部、第 3 の記憶部および第 4 の記憶部の内容をマスター・サーバで一元管理する為のレプリケーション手段と、
を備えることを特徴とするリモート V P N 認証・管理サーバ。

【請求項 4】 クライアント群と I S P (internet service provider) 群との間に設置され、エンド・ツー・エンドの V P N (virtual private network) サービスを提供する V P N 変換装置群をリモートから認証・管理サービスを提供する方法において、
前記クライアント群からのサービス提供への加入申請を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、
前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第 1 の記憶部に前記クライアント毎に登録するステップと、
前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記 V P N 変換装置群の情報を前記第 1 の記憶部に前記クライアント毎に登録するステップと、
前記登録されたクライアント群との通信内容の履歴を第 2 の記憶部に前記クライアント毎に登録するステップ

と、

前記登録された V P N 変換装置群との通信内容の履歴を第 3 の記憶部に前記 V P N 変換装置毎に登録するステップと、
前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第 4 の記憶部に前記クライアント毎に登録するステップと、
前記登録された V P N 変換装置群から認証証の発行要求があった場合、前記 V P N 変換装置群とに認証証を発行するステップと、
前記認証証が発行された V P N 変換装置群から通信宛先への通信の可否について問合せがあった場合、前記通信宛先で前記第 4 の記憶部に前記クライアント毎に登録された前記通信可能宛先情報を検索するステップと、
前記検索結果を前記 V P N 変換装置群に通知するステップと、
前記認証証が発行された V P N 変換装置群からステータス情報を収集するステップと、
前記認証証が発行された V P N 変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行された V P N 変換装置群から所定周期で収集するステップと、
前記認証証が発行された V P N 変換装置群に所定周期のプロブを送信し障害の監視制御を行うステップと、
前記認証証が発行された V P N 変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群にレポートするステップと、
を備えることを特徴とするリモート V P N 認証・管理サービス提供方法。

【請求項 5】 WWWブラウザを具備したクライアント群と I S P (internet service provider) 群との間に設置され、エンド・ツー・エンドの V P N (virtual private network) サービスを提供する V P N 変換装置群をリモートから認証・管理サービスを提供する方法において、
前記クライアント群からのサービス提供の加入申請を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、
前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第 1 の記憶部に前記クライアント毎に登録するステップと、
前記審査結果でサービス可能と判定された前記クライアント群が使用する前記 V P N 変換装置群の情報を前記第 1 の記憶部に前記クライアント毎に登録するステップと、
前記登録されたクライアント群との通信内容の履歴を第 2 の記憶部に前記クライアント毎に登録するステップと、
前記登録された V P N 変換装置との通信内容の履歴を第

3の記憶部に前記VPN変換装置毎に登録するステップと、
前記クライアントが加入申請時、通信宛先を申請した場合、前記通信宛先情報を第4の記憶部に前記クライアント毎に登録するステップと、
前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記クライアント群と前記VPN変換装置群とに認証証を発行するステップと、
前記認証証が発行されたVPN変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第4の記憶部に前記クライアント毎に登録された前記通信宛先情報を検索するステップと、
前記検索結果を前記認証証が発行されたVPN変換装置群に通知するステップと、
前記認証証が発行されたVPN変換装置群からステータス情報を収集するステップと、
前記認証証が発行されたVPN変換装置群でログインしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集するステップと、
前記認証証が発行されたVPN変換装置群に所定周期のプロブを送信し障害の監視制御を行うステップと、
前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポート情報を編集するステップと、
前記所定周期で編集した文書情報を電子メールにハイパーリンクするステップと、
前記電子メールに前記第1の記憶部にある前記クライアント群のメールアドレスを付加するステップと、
前記電子メールを所定周期で送信するステップと、
前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポート内容が表示されるステップと、
を備えることを特徴とするリモートVPN認証・管理サービス提供方法。

【請求項6】 請求項5に記載のリモートVPN認証・管理サービス提供方法において、
地理的条件と前記認証証が発行されたVPN変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散サーバ構成とするステップと、
前記マスター・サーバで前記マスター・サーバと前記スレーブ・サーバとの通信の履歴を第5の記憶部に前記スレーブ・サーバ毎に登録するステップと、
前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証するステップと、

前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバで前記ワン・タイム・パスワードで認証するステップと、
前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバがあった場合、前記マスター・サーバにおいて、最適代替スレーブ・サーバの選択ステップと、
前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象とする前記認証証が発行されたVPN変換装置に関する前記第1の記憶部、第2の記憶部、第3の記憶部および第4の記憶部の関連情報を送信し確認応答をとるステップと、
前記スレーブ・サーバ群には、前記第1の記憶部、第2の記憶部、第3の記憶部および第4の記憶部の内容をマスター・サーバで一元管理する為のレプリケーションステップと、
を備えることを特徴とするリモートVPN認証・管理サービス提供方法。

【請求項7】 クライアント群とISP (internet service provider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群をリモートから認証・管理サービスを提供する方法をコンピュータに実行させるためのプログラムにおいて、前記方法は、
前記クライアント群からのサービス提供への加入申請情報を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、
前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第1の記憶部に前記クライアント毎に登録するステップと、
前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記VPN変換装置群の情報を前記第1の記憶部に前記クライアント毎に登録するステップと、
前記登録されたクライアント群との通信内容の履歴を第2の記憶部に前記クライアント毎に登録するステップと、
前記登録されたVPN変換装置との通信内容の履歴を第3の記憶部に前記VPN変換装置毎に登録するステップと、
前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第4の記憶部に前記クライアント毎に登録するステップと、
前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記クライアント群と前記VPN変換装置群とに認証証を発行するステップと、
前記認証証が発行されたVPN変換装置群から通信宛先

への通信の可否についての問合せがあった場合、前記通信宛先で前記第1の記憶部に登録された前記通信宛先情報を検索するステップと、
前記検索結果を前記VPN変換装置群に通知するステップと、
前記認証証が発行されたVPN変換装置群からステータス情報を収集するステップと、
前記認証証が発行されたVPN変換装置群でログインしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集するステップと、
前記認証証が発行されたVPN変換装置群に所定周期のプロープを送信し障害の監視制御を行うステップと、
前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群にレポートするステップと、
を備えることを特徴とするプログラム。

【請求項8】 WWWブラウザを具備したクライアント群とISP (internet service provider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群をリモートから認証・管理サービスを提供する方法をコンピュータに実行させるためのプログラムにおいて、前記方法は、

前記クライアント群からのサービス提供の加入申請を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、

前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第1の記憶部に前記クライアント毎に登録するステップと、

前記審査結果でサービス可能と判定された前記クライアント群が使用する前記VPN変換装置群の情報を前記第1の記憶部に前記クライアント毎に登録するステップと、

前記登録されたクライアント群との通信内容の履歴を第2の記憶部に前記クライアント毎に登録するステップと、

前記登録されたVPN変換装置との通信内容の履歴を第3の記憶部に前記VPN変換装置毎に登録するステップと、

前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第4の記憶部に前記クライアント毎に登録するステップと、

前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記クライアント群と前記VPN変換装置群とに認証証を発行するステップと、

前記認証証が発行されたVPN変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第1の記憶部に登録された前記通信宛先情

報を検索するステップと、
前記検索結果を前記認証証が発行されたVPN変換装置群に通知するステップと、
前記認証証が発行されたVPN変換装置群からステータス情報を収集するステップと、
前記認証証が発行されたVPN変換装置群でログインしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集するステップと、
前記認証証が発行されたVPN変換装置群に所定周期のプロープを送信し障害の監視制御を行うステップと、
前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポートする情報を編集するステップと、
前記所定周期で編集した文書情報を電子メールにハイパーリンクするステップと、
前記電子メールに前記第1の記憶部にある前記クライアント群のメールアドレスを付加するステップと、
前記電子メールを所定周期で送信するステップと、
前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポート内容が表示されるステップと、
を備えることを特徴とするプログラム。

【請求項9】 請求項8に記載のリモートVPN認証・管理サービス提供方法をコンピュータに実行させるためのプログラムにおいて、前記方法は、

地理的条件と前記認証証が発行されたVPN変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散サーバ構成とするステップと、

前記マスター・サーバで前記マスター・サーバとスレーブ・サーバとの通信の履歴を第5の記憶部に前記スレーブ・サーバ毎に登録するステップと、

前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証するステップと、

前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバが前記ワン・タイム・パスワードで認証するステップと、

前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバがあった場合、前記マスター・サーバにおいて、最適代替スレーブ・サーバの選択ステップと、

前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象と

する前記認証証が発行されたVPN変換装置に関する前記第1の記憶部、第2の記憶部、第3の記憶部および第4の記憶部の関連情報を送信し確認応答をとるステップと、

前記スレーブ・サーバ群には、前記第1の記憶部、第2の記憶部、第3の記憶部および第4の記憶部の内容をマスター・サーバで一元管理する為のレプリケーションステップと、

を備えることを特徴とするプログラム。

【請求項10】 ネットワークで相互に接続された、請求項1又は請求項2に記載のサーバと、前記VPN変換装置群と、前記クライアント端末群と、を備えるリモートVPN認証・管理システムにおいて、

前記VPN変換装置は、

前記サーバに対し認証証の発行要求を送信する手段と、

前記サーバから返信された認証証を記憶する手段と、

前記クライアントからのアクセス要求があった場合、サーバに対し通信の可否を問い合わせる手段と、

前記問い合わせの結果、通信を制限する返信を受信した場合、前記クライアントからの通信要求を拒絶する手段と、

前記問い合わせの結果、通信可能である旨の返信を受信した場合、前記クライアントに前記VPNサービスを提供する手段と、

前記サーバからのステータス問い合わせに対し、ステータス情報を返送する手段と、

前記クライアントへ又はからの通信の履歴を記憶部に登録する手段と、

前記サーバから通信のログ情報の要求を受信時、前記記憶部のクライアントに関する通信のログ情報を返送する手段と、を備え、

前記クライアント端末は、

前記VPN通信手段と、

を備えることを特徴とするリモートVPN認証・管理システム。

【請求項11】 請求項10に記載のリモートVPN認証・管理システムにおいて、

前記VPN変換装置は、

前記問い合わせの結果、通信可能である旨の返信を受信した場合、通信相手先の前記認証証が発行されたVPN変換装置との間で暗号化方式等のネゴシエーションを行う機能と、

を更に備え、

前記クライアント端末は、

前記クライアント端末が通信する宛先の前記VPN変換装置との間でVPN通信の為の暗号化方式等のネゴシエーション手段と、を更に備えることを特徴とするリモートVPN認証・管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

【0002】

【従来の技術】特開2000-341327号公報には、VPN構成方式、インターワークルータ装置、パケット通信方式、データ通信装置およびパケット中継装置について、複数のインターネットプロバイダ(ISP)にまたがる仮想専用線(VPN)を提供する方式として、ISPの入口と出口とに、各々VPN変換システムを配備することにより、複数のISPにまたがるVPNサービスを実現する例が示されている。

【0003】特開2000-244547号公報には、移動端末の認証方式およびVPNの通信方式として、ポータルサイトにアクセス時に付与される秘密鍵情報により、VPNを管理しているサーバにアクセスすることにより、異なるネットワーク間にまたがるVPN通信の方式について述べている。

【0004】特開2000-59357号公報には、VPNサービス構築の方法として、管理サーバにネットワークの使用クライアントのID番号、パスワードを登録し、各クライアントには認証・暗号化ソフトウェアを記憶させたICカードを配布し、アクセス時、管理サーバにて認証およびクライアントを使用できるVPNに割り当てることにより、VPNサービスを提供する方式について述べている。

【0005】

【発明が解決しようとする課題】しかしながら、従来の方式には以下の問題点がある。

【0006】特開2000-341327号公報における、VPN構成方式、インターワークルータ装置、パケット通信方式、データ通信装置およびパケット中継装置においては、VPNはリンク・バイ・リンクで設定され管理運用される為、統合的VPNサービスの管理運営が成されないという第1の問題があった。

【0007】又、特開2000-244547号公報における、移動端末の認証方式およびVPNの通信方式においては、クライアントにICカードを配布し、クライアントの端末には、ICカード・リーダ等の設備を必要とすると共に複数のISPにまたがる通信においては、トンネルサーバの運営管理が一元的に成されていないという第2の問題があった。

【0008】本発明は、これらの問題に鑑み発明されたものであり、統合的VPNサービスの提供を行う運営管理方式およびシステムを提供することを第1の目的とする。

【0009】また、VPNサービスを提供するVPN変換装置の一元的管理・運営を行うサービスを提供することを第2の目的とする。

【0010】

【課題を解決するための手段】本発明の第1の観点によれば、クライアント群とISP(internet service pro

vider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群をリモートから認証・管理サービスを提供するサーバにおいて、前記クライアント群からのサービス提供への加入申請情報を受付・審査後、前記審査結果を前記クライアント群に通知する手段と、前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第1の記憶部に前記クライアント毎に登録する手段と、前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記VPN変換装置群の情報を前記第1の記憶部に前記クライアント毎に登録する手段と、前記登録されたクライアント群との通信内容の履歴を第2の記憶部に前記クライアント毎に登録する手段と、前記登録されたVPN変換装置との通信内容の履歴を第3の記憶部に前記VPN変換装置毎に登録する手段と、前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第4の記憶部に前記クライアント毎に登録する手段と、前記VPN変換装置群に認証証を発行する手段と、前記認証証が発行されたVPN変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第4の記憶部に登録された前記通信宛先情報を検索する手段と、前記検索結果を前記VPN変換装置群に通知する手段と、前記認証証が発行されたVPN変換装置群からステータス情報を収集する手段と、前記認証証が発行されたVPN変換装置群でログインしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集する手段と、前記認証証が発行されたVPN変換装置群に所定周期のプロープを送信し障害の監視制御を行う手段と、前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析する手段と、前記分析結果を前記認証証が発行された前記各クライアント群にレポートする手段と、を備えることを特徴とするリモートVPN認証・管理サーバが提供される。

【0011】本発明の第2の観点によれば、WWWブラウザを具備したクライアント群とISP (internet service provider) 群との間に設置され、エンド・ツー・エンドのVPN (virtual private network) サービスを提供するVPN変換装置群をリモートから認証・管理サービスを提供するシステムにおいて、前記クライアント群からのサービス提供への加入申請情報を受付・審査後、前記審査結果を前記クライアント群に通知する手段と、前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第1の記憶部に前記クライアント毎に登録する手段と、前記審査結果でサービス可能と判定された前記クライアント群が使用する前記VPN変換装置群の情報を前記第1の記憶部に前記

クライアント毎に登録する手段と、前記登録されたクライアント群との通信内容の履歴を第2の記憶部に前記クライアント毎に登録する手段と、前記登録されたVPN変換装置との通信内容の履歴を第3の記憶部に前記VPN変換装置毎に登録する手段と、前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第4の記憶部に前記クライアント毎に登録する手段と、前記登録されたVPN変換装置群から認証証の発行要求があった場合、前記クライアント群と前記VPN変換装置群とに認証証を発行する手段と、前記認証証が発行されたVPN変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第4の記憶部に登録された前記通信宛先情報を検索する手段と、前記検索結果を前記認証証が発行されたVPN変換装置群に通知する手段と、前記認証証が発行されたVPN変換装置群からステータス情報を収集する手段と、前記認証証が発行されたVPN変換装置群でログインしているトラフィックに関する統計情報を、前記認証証が発行されたVPN変換装置群から所定周期で収集する手段と、前記認証証が発行されたVPN変換装置群に所定周期のプロープを送信し障害の監視制御を行う手段と、前記認証証が発行されたVPN変換装置群から収集したトラフィックに関する統計情報を分析する手段と、前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポートする手段と、前記所定周期で編集した文書情報を電子メールにハイパーリンクする手段と、前記電子メールに前記第1の記憶部にある前記クライアント群のメールアドレスを付加する手段と、前記電子メールを所定周期で送信する手段と、前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポート内容が表示される手段と、を備えることを特徴とするリモートVPN認証・管理サーバが提供される。

【0012】前記リモートVPN認証・管理サーバは、地理的条件と前記認証証が発行されたVPN変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散システム構成とする手段と、前記マスター・サーバで前記マスター・サーバとスレーブ・サーバとの通信の履歴を第5の記憶部に前記スレーブ・サーバ毎に登録する手段と、前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証する手段と、前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバで前記ワン・タイム・パスワードで認証する手段と、前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバ

があった場合、前記マスター・サーバにおいて、最適代替スレーブ・サーバの選択手段と、前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象とする前記認証証が発行されたVPN変換装置に関する前記第1の記憶部、第2の記憶部、第3の記憶部および第4の記憶部の関連情報を送信し確認応答をとる手段と、前記スレーブ・サーバ群には、前記第1の記憶部、第2の記憶部、第3の記憶部および第4の記憶部の内容をマスター・サーバで一元管理する為のレプリケーション手段と、を更に備えてもよい。

【0013】本発明の第3の観点によれば、ネットワークで相互に接続された、前記サーバと、前記VPN変換装置群と、前記クライアント端末群と、を備えるリモートVPN認証・管理システムにおいて、前記VPN変換装置は、前記サーバに対し認証証の発行要求を送信する手段と、前記サーバから返信された認証証を記憶する手段と、前記クライアントからのアクセス要求があった場合、サーバに対し通信の可否を問い合わせる手段と、前記問い合わせの結果、通信を制限する返信を受信した場合、前記クライアントからの通信要求を拒絶する手段と、前記問い合わせの結果、通信可能である旨の返信を受信した場合、通信相手先の前記認証証が発行されたVPN変換装置との間で暗号化方式等のネゴシエーションを行う機能と、前記クライアントに前記VPNサービスを提供する手段と、前記サーバからのステータス問い合わせに対し、ステータス情報を返送する手段と、前記クライアントへ又はからの通信の履歴を記憶部に登録する手段と、前記サーバから通信の履歴情報の要求を受信時、前記記憶部のクライアントに関する通信履歴情報を返送する手段と、を備え、前記クライアント端末は、前記VPN通信手段と、前記クライアント端末が通信する宛先の前記VPN変換装置との間でVPN通信の為の暗号化方式等のネゴシエーション手段と、を備えることを特徴とするリモートVPN認証・管理システムが提供される。

【0014】

【発明の実施の形態】実施の形態1について、図1から図4を用いて説明する。

【0015】図1は、本発明のシステム構成を示しており、端末-X101、イントラネット-A102、イントラネット-B103、イントラネット内の端末-A、イントラネット内の端末-B105、VPN変換装置-A106、VPN変換装置-B107、リモートVPN認証・管理サーバ（マスター）108、リモートVPN認証・管理サーバ（スレーブ）109、交換網110、ISP-A111、ISP-X112、ワールドワイドインターネット113から構成される。

【0016】図2は、リモートVPN認証・管理サーバにおける機能構成を示しており、加入者情報記憶部20

1、VPN変換装置情報記憶部202、X.509ディレクトリ記憶部203、加入者通信履歴記憶部204、VPN通信履歴記憶部205、スレーブ通信履歴記憶部（マスター・サーバ）206、VPN変換装置認証機能211、CA発行・登録機能212、X.509ディレクトリ記憶部検索機能213、通信制限制御機能214、VPN変換装置診断・分析機能220、ログ情報収集機能221、スレーブDBレプリケーション機能222、加入者通知機能223、ログ情報分析機能224、分析結果編集機能225、編集文書送信機能226、システム・リコンフィグレーション機能230、スレーブ診断機能（マスター・サーバ）240、スレーブ診断分析機能241、最適代替スレーブ選択機能（マスター・サーバ）242、最適スレーブ・リロケーション機能（マスター・サーバ）243、スレーブ担当情報検索・編集機能（マスター・サーバ）245、対外部送受信機能250から構成される。

【0017】加入者情報記憶部201は、クライアントから加入申請があった場合、クライアントが設置したVPN変換装置がサービス提供対象の仕様を備えているか否かを審査し、サービス提供可能であれば加入を認可し、クライアントが申請したクライアントのメールアドレス、クライアントが設置したVPN変換装置のIPアドレス、サービス料金決済方法、サーバが登録時発行するクライアントのオーガニゼーション番号、ID番号、シグネチャ番号情報を記憶するクライアント毎に記憶する。

【0018】VPN変換装置情報記憶部202は、CAを発行したVPN変換装置に関する情報をクライアント毎に記憶する。

【0019】X.509ディレクトリ記憶部203は、クライアント別にアクセス可能な通信宛先情報を管理し、X.509に準拠したディレクトリー情報を記憶する。

【0020】加入者通信履歴記憶部204は、CAを発行したクライアント群との通信の履歴情報をクライアント毎に記憶する。

【0021】VPN通信履歴記憶部205は、CAを発行したVPN変換装置との通信履歴情報をVPN変換装置毎に記憶する。

【0022】スレーブ通信履歴記憶部（マスター・サーバ）206は、マスター・サーバでスレーブ・サーバ群との通信の履歴を記憶する。

【0023】VPN変換装置認証機能211は、加入認可したVPN変換装置からのアクセス時、認証を行う。

【0024】CA発行・登録機能212は、加入認可したVPN変換装置からのCA（認証証）要求に対し認証証を発行する。

【0025】X.509ディレクトリ記憶部検索機能213は、VPN変換装置からの通信宛先への通信の可否の問い合わせに対し、通信宛先でX.509ディレクトリー記憶部203のクライアント毎の通信宛先情報を検索する。

【0026】通信制限制御機能214は、X.509ディレクトリー記憶部検索の結果、通信の可否をVPN変換装置に返送する。

【0027】VPN変換装置診断・分析機能220は、CAを発行したVPN変換装置群に所定周期でプローブを送信し、ステータス情報をVPN変換装置から収集する。

【0028】ログ情報収集機能221は、VPN変換装置でのトラフィック関連情報等のロギング情報を一定周期でVPN変換装置から収集する。

【0029】スレーブDBレプリケーション機能222は、マスター・サーバで、各記憶部をマスター・サーバで一元管理するためにスレーブ・サーバでの各記憶部のレプリケーション機能を起動させる。

【0030】加入者通知機能223は、VPN変換装置の診断・分析結果、異常と判断した場合、クライアントにその旨通知する。

【0031】ログ情報分析機能224は、収集されたロギング情報を分析する。

【0032】分析結果編集機能225は、各VPN変換装置でのロギング情報を分析した結果を各クライアント別に編集する。

【0033】編集文書送信機能226は、各クライアント別に編集されたレポート情報をハイパーリンクし、各クライアントのメールアドレスを付加して送信する。

【0034】システム・リコンフィグレーション機能230は、サーバ・システム内での障害発生時にシステム構成を自動的に再構成する。

【0035】スレーブ診断機能（マスター・サーバ）240は、マスター・サーバでのスレーブ・サーバの状態情報を所定周期で収集する。

【0036】スレーブ診断分析機能241は、スレーブ・サーバからのステータス情報を分析する。

【0037】最適代替スレーブ選択機能（マスター・サーバ）242は、スレーブ・サーバの代替が必要な場合にマスター・サーバで最適な代替スレーブ・サーバを選択する。

【0038】最適スレーブ・リロケーション機能（マスター・サーバ）243は、代替スレーブ・サーバが選択された場合、当該スレーブ・サーバに必要情報を再配置する。

【0039】スレーブ担当情報検索・編集機能245は、マスター・サーバで代替スレーブ・サーバが選択された場合、当該スレーブ・サーバに必要情報を関連記憶部から検索・収集・編集する。

【0040】対外部送受信機能250は、クライアント、VPN変換装置、マスター・サーバ、スレーブ・サーバ群へ及びからの通信の送受信を行う。

【0041】次に実施の形態1の動作について、図3及び図4を用いて説明する。

【0042】図3において、クライアントからサービス加入申請があった場合（S301）、加入申請情報からサービス提供可能か否かを審査し不可の場合、審査結果を電子メールで通知する（S303）。サービス提供可能である場合には、各クライアントにオーガニゼーション番号、ID番号、シグネチャ番号（パスワード）を発行し送付（S302）し、クライアント毎に記憶するサービス加入者情報記憶部201に登録する。

【0043】また、通信宛先情報はクライアント毎に登録管理するX.509ディレクトリー記憶部に登録される。

【0044】審査の結果サービス提供可能であるとされ、オーガニゼーション番号、ID番号、シグネチャ番号（パスワード）が発行されたクライアントのVPN変換装置から、認証書（CA）の発行要求があった場合（S310）、オーガニゼーション番号、ID番号、シグネチャ番号（パスワード）で認証を行い、NGの場合にはその旨返信し（S312）、OKの場合には認証書をVPN変換装置に返送する（S311）。

【0045】次に図4を用いて、一連の動作について説明する。

【0046】CAを発行されたVPN変換装置から、クライアントからのアクセス要求（S410）に基づく通信宛先との通信の可否の問い合わせを受信した場合（S420）、オーガニゼーション番号、ID番号、シグネチャ番号（パスワード）で認証を行い、NGの場合にはその旨返信し（S421）、認証OKの場合、各クライアント単位で登録管理するX.509ディレクトリー記憶部を通信宛先で検索し、通信宛先情報に登録されている宛先か否かを判定し、判定結果をVPN変換装置に返送し（S422）、通信の制限・制御を行う。

【0047】次にリモートVPN変換装置認証・管理サーバから所定周期でCAを発行されたVPN変換装置群にステータス情報を収集するプローブを送信し（S430）、VPN変換装置群からのステータス情報を添付した返信を受信し（S431）、受信結果を分析し、VPN変換装置に異常が認められた場合、クライアントにその旨通知し（S432）、VPN装置の障害等の監視を行う。

【0048】次にリモートVPN変換装置認証・管理サーバから所定周期でCAを発行されたVPN変換装置群にVPN変換装置群でロギングしているトラフィック関連情報を収集する為のプローブを送信し（S440）、VPN変換装置群からVPN変換装置群でロギングしているトラフィック関連情報を添付した返信を受信し（S441）、VPN装置群のトラフィック関連情報を収集し、収集したトラフィック関連の統計情報を分析する。

【0049】次に分析されたトラフィック関連情報は文書に編集し、各クライアントに編集された文章情報をハイパーリンクしたメールを送信し（S442）、メールを受信した各クライアントは、編集された文章情報を開くと自動的にWWWブラウザが起動され、編集された文章

情報にアクセスし（S443）、WWWブラウザの画面に編集された文章が表示される（S444）。

【0050】第2の実施の形態について、図5を用いて説明する。

【0051】図5に示すように、分散システム構成時、リモートVPN認証・管理スレーブ・サーバ群501に対し、マスター・サーバ108からステータス状況を問い合わせるプローブが所定周期で送信され（S510）、スレーブ・サーバ群501からのステータス情報を含む返信を受信する（S511）。

【0052】次にスレーブ・サーバ群501からの返信情報に過負荷情報、障害情報又は無応答をマスター・サーバ108で検出した場合、マスター・サーバ108は最適な代替スレーブ・サーバを選定し、当該スレーブ・サーバに代替スレーブ指示を送信し（S521）、確認応答を取り（S522）、代替関連情報を当該スレーブ・サーバに送信し（S523）、確認応答（S524）を当該スレーブ・サーバからとることにより、提供サービスに切れ目の無いコンシステンシー・サービスを提供する。

【0053】次にマスター・サーバ108で一元管理する為、所定周期でスレーブ・サーバ群501のレプリケーション機能にスレーブ・サーバの各記憶部の前回送信からの差分の送信要求（S530）を送信し、各記憶部の差分を受信（S531）する動作をすべてのスレーブ・サーバに対し行い、マスター・サーバ108の各記憶部を更新・登録することにより、一元的に全てのVPN変換装置及びサービス提供クライアント情報を管理する。

【0054】第3の実施の形態について、図4及び図6を用いて説明する。

【0055】図4に示した本発明の動作説明図におけるVPN変換装置群402、リモートVPN認証管理サーバ303についての動作については、図4に示した通りである。

【0056】ここでは図6でのイントラネット内の端末-A104とVPN変換装置-A106及びVPN変換装置-B107を介したイントラネット内の端末-B105間での動作について図6にて説明する。

【0057】図6において、VPN変換装置にイントラネット内の端末-A104からアクセス要求（S610）が有ると、図4に示したようにリモート認証管理サーバにアクセスの可否を問い合わせ、アクセス可の場合、宛先イントラネット内の端末-B105のVPN変換装置-B107にVPN変換装置-A106からアクセス（S611）し、IPsecに基づく暗号化方式等のネゴシエーション（S612）をVPN変換装置間（106、107）で行い（S612）、VPNセッション確立後、端末-A104と端末-B105間でVPN通信（S613）を行う。

【0058】次に、図7を用いて端末にVPN通信機能を搭載した場合での動作について説明する。

【0059】図7において、端末-X101からISP-X112にダイヤルアップ回線接続（S710）を行い予め加入契約したISP-X112の接続ポートと接続し、ID、パスワードの送信（S711）によりISP-X112から認証を受け、IPアドレスが返送（S712）される。

【0060】接続宛先端末-A104のVPN変換装置-A106に通信要求を送信（S713）し、IPsecに基づく暗号化方式等のネゴシエーション（S714）をVPN変換装置-A106との間で行いVPNセッション確立後、VPN通信（S715）にて端末-X101と端末-A104の間でVPNを使用した通信を行う。

【0061】

【発明の効果】本発明の第1の効果は、エンド・ツー・エンドでシンプルかつメンテナンス・フリーなVPN変換装置の認証・管理サービスが提供されることである。

【0062】本発明の第2の効果は、従来1つのISPに閉じられていたVPNサービスとその認証・管理に統合的なサービスが提供されることである。

【0063】本発明の第3の効果は、従来1つのISPに閉じられていたVPNサービスとその認証・管理に一元的な管理サービスが提供されることである。

【0064】本発明の第4の効果は、分散型システム構成をとることにより、信頼性の高いサービスが提供されることである。

【0065】本発明の第5の効果は、また、分散型のシステムにより、VPN変換装置との間のトラフィックを軽減できることである。

【0066】本発明の第6の効果は、分散型のシステム構成をとることにより、スレーブ・サーバの初期投資を軽減できることである。

【図面の簡単な説明】

【図1】本発明のシステム構成概要を示すシステム構成概要図である。

【図2】本発明のサーバでの機能構成と機能間の関連を示すシステム機能構成図である。

【図3】本発明のクライアントから加入申請を受けてから、CAを発行するまでのクライアント、VPN変換装置及びリモート認証管理サーバ間の動作を示すシーケンス図である。

【図4】本発明でのCAを発行されたクライアント、VPN変換装置及びリモート認証管理サーバ間の動作を示すシーケンス図である。

【図5】本発明のシステム構成を分散システム構成とした場合のマスター・サーバとスレーブ・サーバ群との動作を示すシーケンス図である。

【図6】本発明のVPN変換機能搭載の端末及びVPN変換装置を介したイントラネット内の端末間での通信でのシ

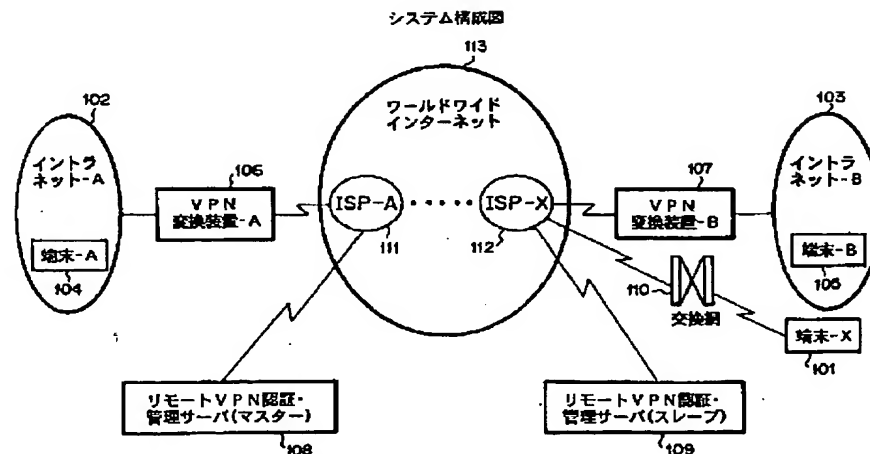
テム構成と各システムの動作を示すシーケンス図である。

【図7】本発明のイントラネット内の端末間でVPN通信を行う場合のシステム構成と各システムでの動作について示すシーケンス図である。

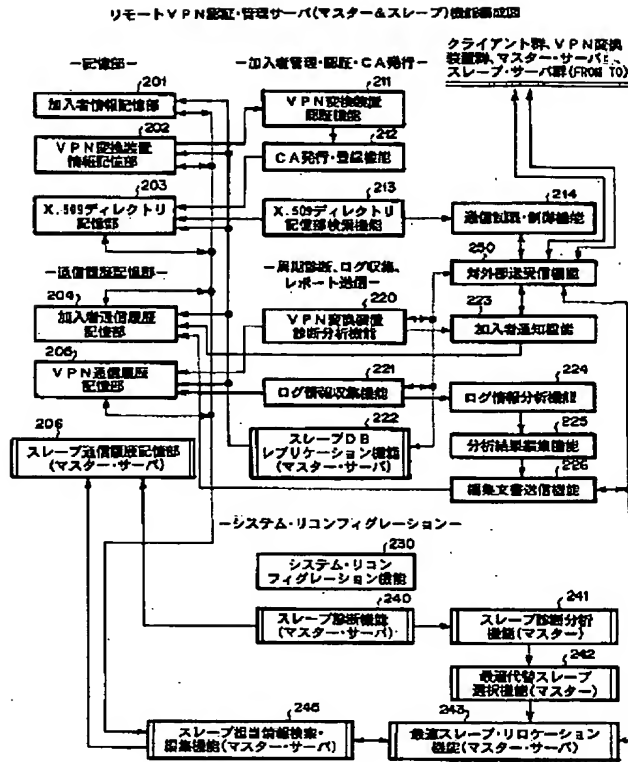
【符号の説明】

- | | | | |
|-----|-----------------------|-----|----------------------------|
| 101 | 端末-X | 212 | CA発行・登録機能 |
| 102 | イントラネット-A | 213 | X.509ディレクトリ記憶部検索機能 |
| 103 | イントラネット-B | 214 | 通信制限制御機能 |
| 104 | イントラネット内の端末-A | 220 | VPN変換装置診断・分析機能 |
| 105 | イントラネット内の端末-B | 221 | ログ情報収集機能 |
| 106 | VPN変換装置-A | 222 | スレーブDBレプリケーション機能 |
| 107 | VPN変換装置-B | 223 | 加入者通知機能 |
| 108 | リモート認証管理サーバ(マスター・サーバ) | 224 | ログ情報分析機能 |
| 109 | リモート認証管理サーバ(スレーブ・サーバ) | 225 | 分析結果編集機能 |
| 110 | 交換網 | 226 | 編集文書送信機能 |
| 111 | ISP-A | 230 | システム・リコンフィグレーション機能 |
| 112 | ISP-X | 240 | スレーブ診断機能(マスター・サーバ) |
| 113 | ワールドワイドインターネット | 241 | スレーブ診断分析機能 |
| 201 | 加入者情報記憶部 | 242 | 最適代替スレーブ選択機能(マスター・サーバ) |
| 202 | VPN変換装置情報記憶部 | 243 | 最適スレーブ・リロケーション機能(マスター・サーバ) |
| 203 | X.509ディレクトリ記憶部 | 245 | スレーブ担当情報検索・編集機能(マスター・サーバ) |
| 204 | 加入者通信履歴記憶部 | 250 | 対外部送受信機能 |
| 205 | VPN通信履歴記憶部 | 301 | クライアント |
| 206 | スレーブ通信履歴記憶部(マスター・サーバ) | 302 | VPN変換装置 |
| 211 | VPN変換装置認証機能 | 303 | リモート認証管理サーバ |
| | | 401 | クライアント群 |
| | | 402 | VPN変換装置群 |
| | | 501 | スレーブ・サーバ群 |

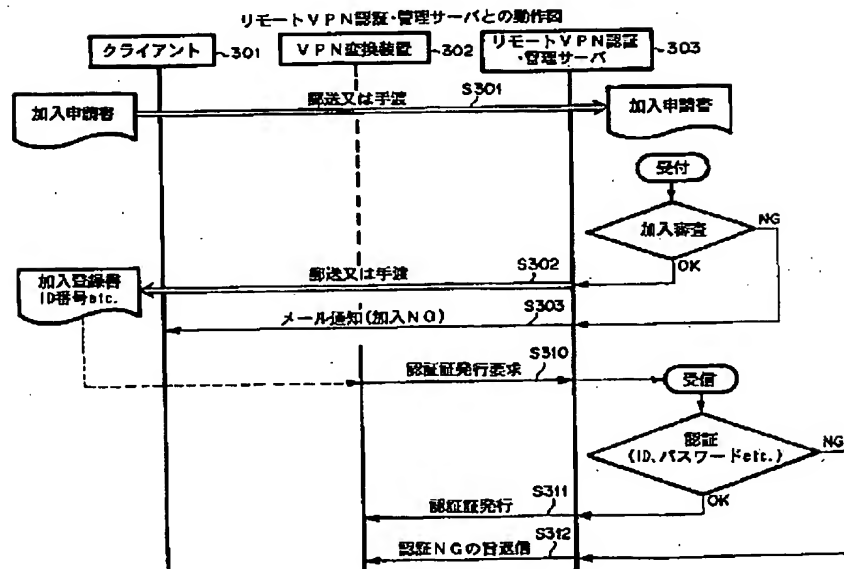
【図1】



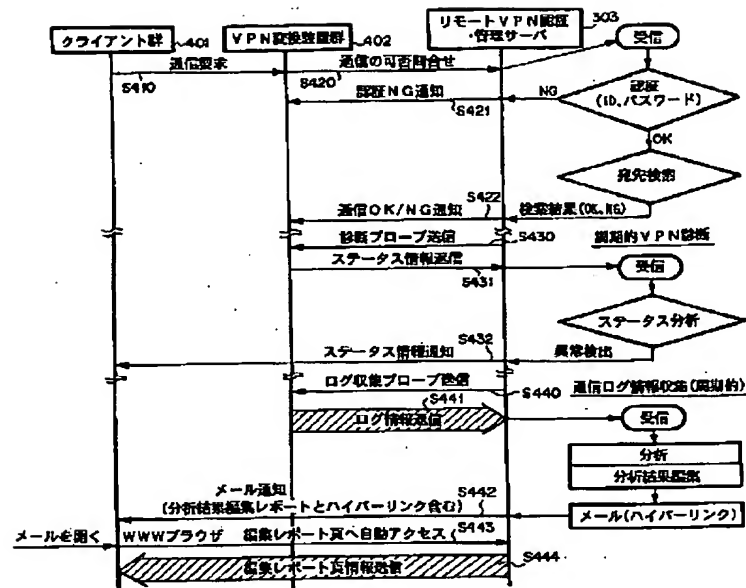
【図2】



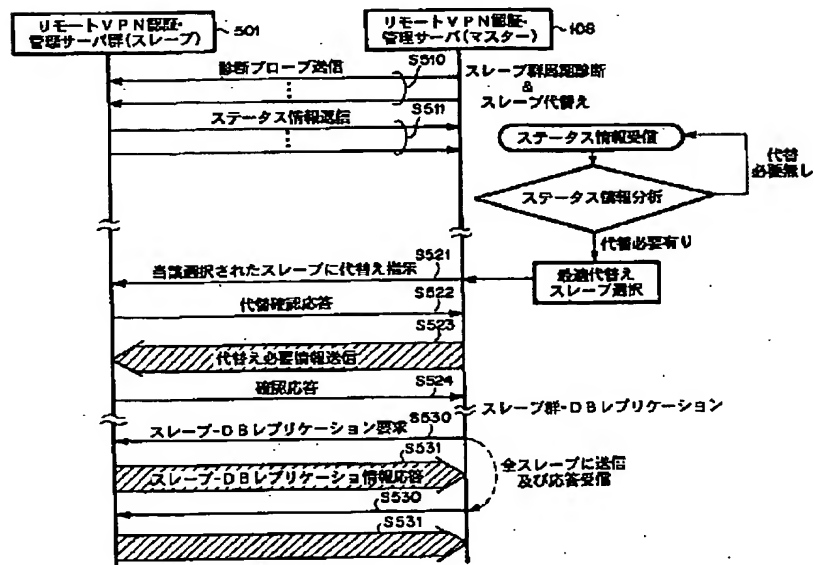
【図3】



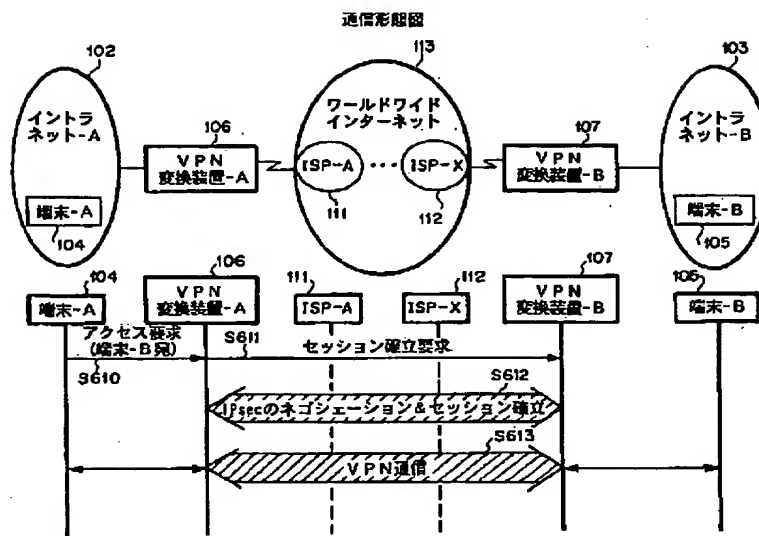
【図4】



【図5】



【図6】



【図7】

